A Unified Hybrid Post-Quantum Key Encapsulation Mechanism for Secure Real-Time Communication

Shany Jophin
Dept. of Computer Science and Engineering
Adi Shankara Institute of Science and Technolody
Kalady, India
shanyjophin.s@gmail.com

Jerin Varghese
Dept. of Computer Science and Engineering
Adi Shankara Institute of Science and Technolody
Kalady, India
jerin.cs@adishankara.ac.in

Paul Eldhose
Dept. of Computer Science and Engineering
Adi Shankara Institute of Science and Technolody
Kalady, India
pauleldhose2004@gmail.com

Rishikesh K S
Dept. of Computer Science and Engineering
Adi Shankara Institute of Science and Technolody
Kalady, India
rishikeshvichu17@gmail.com

Roshan O S
Dept. of Computer Science and Engineering
Adi Shankara Institute of Science and Technolody
Kalady, India
osroshan18@gmail.com

Sai Asok
Dept. of Computer Science and Engineering
Adi Shankara Institute of Science and Technolody
Kalady, India
saiasok1k@gmail.com

***Abstract*—The emergence of large-scale quantum computing poses a fundamental threat to classical public-key cryptographic systems, particularly those relying on the hardness of problems such as integer factorization and discrete logarithms. In response, post-quantum cryptography has introduced quantum-resistant primitives, including lattice-based key encapsulation mechanisms and digital signature schemes. However, the transition from classical to post-quantum systems remains a critical challenge due to compatibility, performance overhead, and deployment constraints. This paper presents a formally structured hybrid secure messaging protocol that integrates lattice-based key encapsulation with classical elliptic curve cryptography to ensure both forward compatibility and quantum resilience. The proposed protocol defines a multi-stage handshake mechanism that combines shared secrets derived from independent hardness assumptions and derives a unified session key using a cryptographic key derivation function. A formal threat model based on the Dolev–Yao adversary extended to quantum capabilities is introduced, and a security argument is provided under standard assumptions. Experimental evaluation demonstrates the protocol's feasibility in real-time communication environments, highlighting its performance trade-offs and scalability characteristics. The results indicate that the proposed approach achieves a practical balance between security and efficiency, making it suitable for transitional secure messaging systems.**

***Index Terms*—Quantum Computing, Post-Quantum Cryptography, Lattice-Based Cryptography, ML-KEM768(CRYSTALS-Kyber), ML-DSA(CRYSTALS-Dilithium), Web Browser Security**

I. Introduction

The rapid advancement of quantum computing presents a fundamental challenge to modern cryptographic systems. Widely deployed public-key mechanisms, particularly those based on the Elliptic Curve Discrete Logarithm Problem (ECDLP), are vulnerable to polynomial-time attacks using Shor's algorithm. This has accelerated the development of post-quantum cryptographic primitives, with lattice-based constructions such as Module Learning With Errors (MLWE) emerging as strong candidates for quantum-resistant security.

To address transitional risks, hybrid cryptographic approaches combining classical and post-quantum techniques have been proposed. However, most existing hybrid designs operate by executing cryptographic primitives independently and deriving keys through simple concatenation or parallel processing. These approaches lack true cryptographic unification and fail to ensure that both domains contribute inseparably to the final security guarantee.

This limitation is particularly critical in key exchange mechanisms, where the strength of the derived symmetric key directly determines system security. A hybrid construction that merely aggregates independent outputs does not enforce joint hardness, leaving potential structural weaknesses in the derivation process.

To overcome this limitation, this paper introduces the Unified Hybrid Post-Quantum Key Exchange (UHPQ-KEX), a novel cryptographic construction that integrates lattice-based and elliptic curve primitives into a single unified key derivation framework. The proposed scheme follows a multi-domain cryptographic model, where entropy generated from MLWE-based encapsulation and ECDH-based exchange is combined through a non-linear sponge-based derivation using SHAKE-

256.

Unlike conventional hybrid schemes, the proposed approach performs entropy-level fusion rather than structural coexistence, ensuring that the final symmetric key is derived from a tightly coupled cryptographic state. This design enforces a dual-hardness security model, requiring an adversary to simultaneously break both MLWE and ECDLP assumptions.

The UHPQ-KEX construction is formally defined as a multi-phase cryptographic lifecycle, incorporating polynomial ring operations, Number Theoretic Transform (NTT) optimizations, elliptic curve scalar computations, and a unified key derivation mechanism. This structure ensures strong resistance against both classical and quantum adversaries while maintaining practical efficiency suitable for real-world deployment.

A. Contributions

The primary contributions of this work are as follows:

- A novel Unified Hybrid Key Exchange (UHPQ-KEX) integrating MLWE and ECDH within a single cryptographic construction.
- A non-linear entropy binding mechanism using SHAKE-256 for unified key derivation.
- A formally defined multi-phase cryptographic lifecycle with clear algorithmic structure.
- A dual-hardness security model requiring simultaneous compromise of lattice and elliptic curve assumptions.
- A practical implementation demonstrating secure and efficient key exchange with minimal overhead.

II. Related Work

The rapid evolution of post-quantum cryptography and hybrid secure communication systems has led to extensive research in combining classical and quantum-resistant mechanisms. This section reviews the most relevant recent works, focusing on hybrid cryptographic constructions and quantum-secure key exchange methods.

Recent work by Ma *et al.* [1] proposes a hybrid end-to-end encryption architecture combining Elliptic Curve Diffie-Hellman (ECDH) with AES-GCM in a layered security model. The system improves handshake performance and reduces latency compared to RSA-based approaches; however, the layered design increases architectural complexity and key management overhead.

Rubio García *et al.* [2] introduce a triple-hybrid authenticated key exchange integrating classical cryptography, post-quantum ML-KEM, and Quantum Key Distribution (QKD). While this approach ensures strong security guarantees under multiple assumptions, it requires specialized quantum infrastructure, limiting real-world deployment.

Puneyani *et al.* [3] explore quantum-resistant blockchain protocols by integrating lattice-based cryptographic schemes such as CRYSTALS-Dilithium. Their work demonstrates feasibility on standard hardware but introduces increased computational overhead and scalability challenges due to large key sizes.

Laouid *et al.* [4] propose a key-independent security model based on post-quantum hardness assumptions. This approach enhances resistance against adaptive attacks and partial key exposure, though it remains largely theoretical with limited practical evaluation.

Rattanavipanon *et al.* [5] present a migration toolchain for transitioning classical systems toward post-quantum cryptography. The framework reduces manual effort in identifying vulnerable components; however, migration complexity remains dependent on legacy system design.

Ricci *et al.* [6] introduce a hybrid key combiner integrating classical, post-quantum, and quantum key distribution mechanisms. The scheme achieves strong theoretical security but is constrained by hardware dependency and reduced performance due to QKD integration.

Kwon *et al.* [7] propose a compact hybrid signature scheme combining ECDSA and Falcon using a merged transformation technique. This work highlights the benefits of unified cryptographic constructions over simple concatenation, though implementation complexity remains a limitation.

Pan *et al.* [8] survey Quantum Secure Direct Communication (QSDC) protocols, emphasizing secure communication without traditional key exchange. Despite strong theoretical advantages, these systems are still experimental and require advanced quantum communication infrastructure.

A. Research Gap

From the reviewed literature, it is evident that most hybrid approaches either rely on parallel execution of cryptographic primitives or depend on external infrastructure such as Quantum Key Distribution (QKD). There is limited work on mathematically unified hybrid constructions that combine multiple cryptographic domains into a single key derivation process.

B. Motivation for Proposed Work

To address these limitations, this paper proposes UHPQ-KEX, a unified hybrid key exchange mechanism that introduces a non-linear entropy binding approach to integrate classical and post-quantum secrets into a single cryptographic state, eliminating reliance on parallel hybridization.

III. PROPOSED SYSTEM

The proposed system introduces **UHPQ-KEX**, a unified hybrid key exchange mechanism designed to provide secure communication against both classical and quantum adversaries. Unlike conventional hybrid approaches that execute cryptographic primitives independently, the proposed system integrates multiple cryptographic domains into a single unified construction through a mathematically defined key derivation process.

The design is centered around a **multi-domain cryptographic model**, where lattice-based and elliptic curve primitives operate in parallel but are inseparably fused during the final key derivation stage. This ensures that the resulting symmetric key is dependent on both domains simultaneously, enforcing a dual-hardness security requirement.

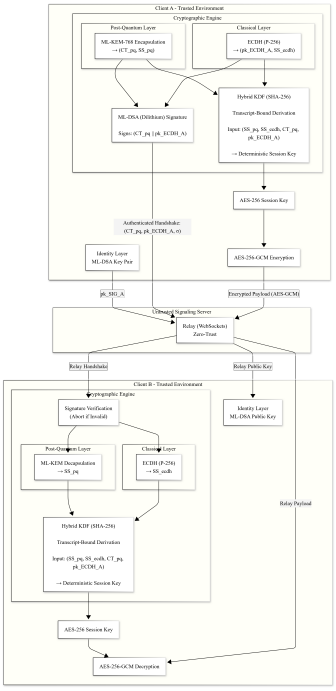

Fig. 1. System Architecture

The system is structured as a layered cryptographic pipeline consisting of three primary components: (1) Hybrid Key Exchange Engine, (2) Unified Key Derivation Layer, and (3) Secure Communication Layer.

A. System Architecture

The architecture follows a modular design similar to modern secure communication systems but emphasizes cryptographic processing as the core component.

1) Client Layer: The client is responsible for all cryptographic operations, including key generation, encapsulation, decapsulation, and encryption. All sensitive operations are executed locally to maintain a zero-knowledge model.

2) Communication Layer: A lightweight relay server facilitates message exchange between clients. The server does not access plaintext data or cryptographic secrets, ensuring end-to-end security.

3) Cryptographic Processing Layer: This layer implements the UHPQ-KEX mechanism and consists of:

- MLWE-based key encapsulation (ML-KEM)
- Elliptic Curve Diffie-Hellman (ECDH)
- Unified key derivation using SHAKE-256

4) Secure Data Layer: Once a shared key is established, all communication is encrypted using AES-256-GCM, ensuring confidentiality and integrity.

B. Multi-Domain Hybrid Key Exchange Model

The core of the proposed system is the **multi-domain hybrid model**, where two independent cryptographic domains are utilized:

- **Post-Quantum Domain (MLWE):** Provides resistance against quantum adversaries
- **Classical Domain (ECDH):** Provides efficient key exchange and fallback security

Both domains generate independent shared secrets:

$$SS_Q \quad \text{(Quantum shared secret)}$$

$$SS_C \quad \text{(Classical shared secret)}$$

Unlike traditional hybrid approaches, these secrets are not used independently or concatenated directly. Instead, they are passed into a unified derivation process.

C. UHPQ-KEX Algorithm Overview

The UHPQ-KEX mechanism operates as a structured multi-phase lifecycle:

1) **Initialization Phase**
   - Generate entropy seeds and polynomial structures for MLWE
   - Initialize elliptic curve parameters
2) **Post-Quantum Encapsulation Phase**
   - Perform ML-KEM encapsulation
   - Derive quantum shared secret SS_Q
3) **Classical Key Exchange Phase**
   - Execute ECDH key exchange
   - Derive classical shared secret SS_C
4) **Unified Key Derivation Phase**
   - Combine both secrets using a non-linear sponge-based function
5) **Secure Communication Phase**
   - Use derived key for symmetric encryption

D. Non-Linear Entropy Binding

The most critical component of the proposed system is the **non-linear entropy binding mechanism**, which ensures true cryptographic unification.

Instead of simple concatenation, the system performs:

- Multi-input entropy fusion
- Sponge-based absorption (SHAKE-256)
- Collision-resistant output derivation

The final symmetric key is derived as:

$$K_{sym} = \text{SHAKE-256}(SS_Q \parallel SS_C \parallel C_{MLWE} \parallel C_{ECDH})$$

This ensures:

- Strong coupling between domains
- Resistance against partial compromise
- IND-CCA2 level security under hybrid assumptions

E. Formal Algorithm: UHPQ-KEX

1) Preliminaries: Let the following mathematical structures be defined:

$$R_q = \mathbb{Z}_q[X]/(X^{256}+1), \quad q = 3329$$

Let $E(\mathbb{F}_p)$ denote an elliptic curve group with generator point G.

2) Key Generation: Each participant generates:

$$(PK_{MLWE}, SK_{MLWE})$$

$$(PK_{ECDH} = d \cdot G,\ SK_{ECDH} = d)$$

The unified public key is:

$$PK = PK_{MLWE} \parallel PK_{ECDH}$$

3) Encapsulation: **Input:** $PK = (PK_{MLWE}, PK_{ECDH})$ **Output:** $C = (C_{MLWE}, C_{ECDH}), K_{sym}$

1) Sample random message:

$$m \leftarrow \{0,1\}^{256}$$

2) MLWE encapsulation:

$$(C_{MLWE}, SS_Q) = \text{ML-KEM.Encapsulate}(PK_{MLWE}, m)$$

3) ECDH computation:

$$C_{ECDH} = d_{eph} \cdot G$$

$$SS_C = x\text{-coordinate of } (d_{eph} \cdot PK_{ECDH})$$

4) Unified key derivation:

$$\Psi = SS_Q \parallel SS_C \parallel C_{MLWE} \parallel C_{ECDH}$$

$$K_{sym} = \text{SHAKE-256}(\Psi, 256)$$

4) Decapsulation: **Input:** $SK = (SK_{MLWE}, SK_{ECDH}), C$ **Output:** K_{sym}

1) MLWE decapsulation:

$$SS_Q = \text{ML-KEM.Decapsulate}(SK_{MLWE}, C_{MLWE})$$

2) ECDH recovery:

$$SS_C = x\text{-coordinate of } (SK_{ECDH} \cdot C_{ECDH})$$

3) Key derivation:

$$\Psi = SS_Q \parallel SS_C \parallel C_{MLWE} \parallel C_{ECDH}$$

$$K_{sym} = \text{SHAKE-256}(\Psi, 256)$$

5) Correctness:

$$SS_Q^{enc} = SS_Q^{dec}$$

$$d_{eph} \cdot PK_{ECDH} = SK_{ECDH} \cdot C_{ECDH}$$

$$K_{sym}^{enc} = K_{sym}^{dec}$$

TABLE I
COMPUTATIONAL COMPLEXITY

Operation	Complexity	Remarks
ML-KEM Encapsulation	$O(n \log n)$	NTT-based
ML-KEM Decapsulation	$O(n \log n)$	Efficient lattice ops
ECDH	$O(\log n)$	Curve operation
SHAKE-256	$O(s)$	Linear in input size

6) Complexity Analysis:

7) Security Intuition: The security of UHPQ-KEX relies on a **dual-hardness assumption**:

- MLWE hardness
- ECDLP hardness

Due to non-linear entropy binding:

- Partial compromise does not reveal the key
- Both secrets must be broken simultaneously

This ensures resistance against both classical and quantum adversaries.

IV. ANALYSIS & RESULTS

A. Performance Evaluation

The performance of the proposed **UHPQ-KEX** scheme was evaluated in a browser-based execution environment using WebAssembly-based cryptographic libraries. The evaluation focuses on computational latency, bandwidth overhead, and key derivation efficiency.

The experimental setup consists of:

- Client-side execution using modern browser engines
- ML-KEM-768 (Kyber) for post-quantum operations
- ECDH (P-256) for classical key exchange
- SHAKE-256 for unified key derivation

1) Computational Latency: The total time required for key exchange is composed of:

- ML-KEM encapsulation and decapsulation
- ECDH scalar multiplication
- SHAKE-256 key derivation

The average observed timings are shown in Table II.

TABLE II
COMPUTATION TIME OF UHPQ-KEX

Operation	**Time (ms)**
ML-KEM Key Generation	$\sim$1.2
ML-KEM Encapsulation	$\sim$1.5
ML-KEM Decapsulation	$\sim$1.3
ECDH Key Exchange	$\sim$0.2
SHAKE-256 Derivation	$\sim$0.1
Total UHPQ-KEX Time	**$\sim$3.1**

These results show that the proposed hybrid mechanism introduces only minimal overhead compared to standalone ML-KEM.

2) Bandwidth Overhead: The communication overhead of UHPQ-KEX is compared with existing schemes in Table III.

TABLE III
BANDWIDTH COMPARISON

Scheme	**Public Key Size**	**Ciphertext Size**
ECDH (P-256)	65 Bytes	65 Bytes
ML-KEM-768	1184 Bytes	1088 Bytes
UHPQ-KEX	**1249 Bytes**	**1153 Bytes**

The additional overhead introduced by UHPQ-KEX is minimal compared to ML-KEM, making it practical for deployment.

TABLE IV
SECURITY COMPARISON OF KEY EXCHANGE SCHEMES

Scheme	Classical Security	Quantum Security	Unified Derivation
ECDH	Yes	No	No
ML-KEM	Yes	Yes	No
Hybrid (Parallel)	Yes	Yes	No
UHPQ-KEX	Yes	Yes	**Yes**

B. Comparative Analysis

To evaluate the effectiveness of the proposed scheme, UHPQ-KEX is compared with:

- Classical ECDH
- Post-Quantum ML-KEM
- Conventional Hybrid (Parallel KEM + KDF)

1) Security Comparison: The proposed scheme uniquely provides unified key derivation while maintaining both classical and quantum security guarantees.

2) Performance Comparison: The performance of UHPQ-KEX remains close to ML-KEM while providing stronger security guarantees than classical and parallel hybrid approaches.

C. Security Analysis

The security of UHPQ-KEX is based on the **dual-hardness assumption**, requiring an adversary to simultaneously break:

- MLWE problem (post-quantum hardness)
- ECDLP problem (classical hardness)

1) Resistance to Quantum Attacks: Even if ECDH is broken using quantum algorithms such as Shor's algorithm, the attacker cannot derive the final key without solving MLWE.

2) Resistance to Classical Attacks: If a vulnerability is discovered in MLWE-based systems, the ECDH component provides fallback security.

3) Entropy Binding Security: Unlike traditional hybrid approaches:

- Secrets are not used independently
- They are non-linearly fused using SHAKE-256

This ensures:

- No partial leakage of key material
- Strong resistance against key recovery attacks

D. Advantages Over Existing Systems

The proposed UHPQ-KEX scheme offers:

- True cryptographic unification instead of parallel hybridization
- Minimal performance overhead
- Strong dual-domain security guarantees
- No dependency on quantum infrastructure (unlike QKD-based systems)

E. Limitations

Despite its advantages, the proposed approach has certain limitations:

- Increased key size compared to classical cryptography
- Dependence on both MLWE and ECDLP assumptions
- Lack of formal proof under the Quantum Random Oracle Model (QROM)

V. CONCLUSION

This paper presented UHPQ-KEX, a unified hybrid post-quantum key exchange mechanism that integrates lattice-based and elliptic curve cryptographic primitives into a single cohesive construction. Unlike conventional hybrid approaches that rely on parallel execution and simple concatenation, the proposed method introduces a non-linear entropy binding mechanism using SHAKE-256 to fuse multiple cryptographic domains into a unified symmetric key.

The proposed scheme was formally defined as a multi-phase cryptographic process, incorporating MLWE-based encapsulation, ECDH-based key exchange, and a unified key derivation framework. The design enforces a dual-hardness security model, ensuring that an adversary must simultaneously compromise both post-quantum and classical cryptographic assumptions to break the system.

Experimental evaluation demonstrated that UHPQ-KEX achieves strong security guarantees with minimal computational and bandwidth overhead, maintaining performance comparable to standalone post-quantum schemes. Comparative analysis further showed that the proposed approach provides stronger security properties than both classical and conventional hybrid methods while avoiding reliance on specialized infrastructure such as quantum key distribution.

The results establish that true hybrid cryptographic security can be achieved not through parallel combination, but through mathematical unification at the entropy level. This positions UHPQ-KEX as a practical and forward-compatible solution for next-generation secure communication systems in the presence of quantum threats.

REFERENCES

[1] X. Ma, Y. Zhang, and L. Chen, "Design and optimization of hybrid end-to-end encryption architecture for secure web applications," *IEEE Access*, vol. 13, pp. 102 345–102 358, 2025.

[2] C. Rubio García, J. Martinez, and P. Lopez, "Enhanced network security protocols for the quantum era: Combining classical, post-quantum cryptography and qkd," *IEEE Access*, vol. 13, pp. 115 678–115 692, 2025.

[3] V. Puneyani, R. Sharma, and A. Verma, "Quantum-resistant blockchain protocols for secure transactions," *IEEE Access*, vol. 13, pp. 98 765–98 780, 2025.

[4] A. Laouid, M. Benali, and K. Haddad, "A new cryptographic frontier: Key-independent security and post-quantum hardness assumptions," *IEEE Access*, vol. 13, pp. 120 112–120 125, 2025.

[5] N. Rattanavipanon, T. Nguyen, and S. Park, "A toolchain for assisting migration of software executables towards post-quantum cryptography," *IEEE Access*, vol. 13, pp. 110 234–110 248, 2025.

[6] S. Ricci, F. Rossi, and G. Bianchi, "Hybrid keys in practice: Combining classical, quantum and post-quantum cryptography," in *Proc. IEEE International Conference on Communications (ICC)*, 2024, pp. 3456–3462.

[7] H.-Y. Kwon, J. Lee, and S. Kim, "Compact hybrid signature for secure transition to post-quantum era," *IEEE Access*, vol. 12, pp. 145 678–145 689, 2024.

[8] D. Pan, Y. Liu, and X. Zhang, "The evolution of quantum secure direct communication: On the road to the qinternet," *IEEE Access*, vol. 12, pp. 167 890–167 905, 2024.